The defence hub

Earlier this year, eHosting DataFort (eHDF) together with Netcure and LogRhythm launched a Cyber Defense Centre (CDC) in the UAE. Yasser Zeineldin, CEO, eHosting DataFort and Jeff Ogden, Managing Director, eHDF Cyber Defense Centre, discuss CDC's objectives and future plans for the region.

Can you please tell us your objectives behind launching the Cyber Defense Centre?

Yasser Zeineldin (YZ): The Cyber Defense Centre was launched in May this year. It aims to offer customers a range of Managed Security Services (MSS) and Remote Managed SIEM Services.

eHDF as a company has been in the managed services business since 2002, offering 24/7 management for critical customer infrastructure. With the rise of security threats globally and here in the region we thought it's very important to ensure that our customers in the Middle East specifically here in the GCC to have access to state-of-the-art security services and support.

We felt that there was a gap in that space during the previous years. There are a lot of resellers and distributors of security products present in the market. However, when it comes to managing and responding to threats in real-time there are only a few organisations that provide those services. Moreover, what typically happens is that the organisations that provide those services also rely on security operations centres overseas. The customers will then have to wait for those operations centres to get back to them only to find out that they will only be given a set of recommended steps to address the threats. We felt that that was a very ineffective system because from a security perspective they shouldn't leave the response part to the customers. This is because your customers aren't security experts and they may find it challenging to put your recommendations into action. With our legacy as a 24/7 managed services provider, this is an area we excel at.

Yasser Zeineldin, eHDF

So that's the market gap we intend to fill with the new Cyber Defense Centre.

What are the primary security challenges that you aim to address through the new Centre?

YZ: A lot of our customers have been experiencing increased activities in ransomware and DDoS attacks. There are also significant cases of data leakage here in the

region, which happens through a malware penetration prompting the communication of data outside the organisation.

We have also seen a significant number of cases of employee related data leakage. In fact, several industry studies have shown that 59 percent of employees tend to leak corporate data after they leave a company. That's a lot of intellectual property leaking out of organisations, which can have serious implications for a business.

Another driver we have for establishing the CDC is the absence of skills in the market. What we have been seeing is that many customers are buying certain solutions but they don't have the necessary expertise or talent to properly utilise the tools that they have. We can provide them assistance on that front.

Can you please give us an overview of the kind of services you offer at the CDC?

Jeff Ogden (JO): Our key focus is mainly on giving customers the visibility of what's going on within their infrastructures either globally or locally. So what we have done is launched a service called real-time threat monitoring (RTTM). What that service does is collect all the data from a customer's network and bring those data into a centre point, which is the SIEM solution. Our analysts will then take a look at it and evaluate whether it's safe or there are indications of threats in that data. After which, they will alert the customer on the end result and make a decision to mitigate any threats on the customer's behalf.

The RTTM platform is something that we have invested significantly in. Some of our customers have already bought that technology and have it on their sites. Through the platform, we can import their data into our data centres in the UAE and do the analytics for our customers. We believe that you can't manage what you can't measure. So the first step is always to measure everything. Take the data, analyse it and only then can you help your customers secure it and make long-term strategic decisions regarding that data.

The second offering that we have is the Remote Managed SIEM Services (RMSS), which does the same processes as the RTTM but for an on-premise implementation. So if a customer doesn't want to buy the technology they can get in touch with our analysts to examine their data and do the same analytics for them from our data centre.

Apart from managing mission critical applications we also do other security and data protection services as well. We do things like firewall management, DDoS protection and web application protection among others. We have already invested on those components and we deliver them as managed services.

Other vendors in the market may provide customers with the monitoring solutions but they don't usually provide all the support services around that; whereas with eHDF we have around 25 to 30 people working within our security and network operations and we provide all the peripheral services that customers want.

What are your plans over the next few months? Will you be launching new solutions and services?

JO: Going forward we plan to launch two to three other services through the CDC. A lot of customers are struggling with cloud security and

Jeff Ogden, eHDF Cyber Defense Centre

soon we will introduce a cloud access security platform (CASP). This will enable organisations to control the access of users' devices to cloud platforms like Office 365, Salesforce.com and so on. This will allow us to monitor and secure those applications and prevent any data loss.

The second service we'd like to introduce in the coming months is centred on encryption. Various customers today have growing concerns over sending unencrypted data out of their organisations. So, depending on policies, we can encrypt any data that leaves the organisation to make sure that if it does fall into the wrong hands they won't be able to access it. Traditionally that's an on-premise solution they have to buy a certain technology and install it into their systems but with our offering, it'll be very easy to deploy from the cloud.

Those are among the two services we aim to releases soon and you can expect more from us over the next few months.